

The opinion in support of the decision being entered today
is *not* binding precedent of the Board.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte A-JUNG KIM

Appeal 2007-2437
Application 09/816,080
Technology Center 2100

Decided: September 26, 2007

Before JOSEPH L. DIXON, ROBERT E. NAPPI, and
JOHN A. JEFFERY, *Administrative Patent Judges*.
DIXON, *Administrative Patent Judge*.

DECISION ON APPEAL

This is a decision on appeal under 35 U.S.C. § 134 from the Examiner's final rejection of claims 1-6. We have jurisdiction under 35 U.S.C. § 6(b). An Oral Hearing was held on September 11, 2007.

We AFFIRM-IN-PART.

BACKGROUND

Appellant's invention relates to a key agreement method in secure communication system using multiple access method. An understanding of the invention can be derived from a reading of exemplary claim 1, which is reproduced below.

1. A key agreement method for secure communication in a multiple access system, the key agreement method comprising the steps of:
 - (a) a first user encoding a signal from a source by a bit sequence and transmitting the signal;
 - (b) a second user who is a legitimate counterpart of the first user decoding the transmitted signal and measuring the decoded signal;
 - (c) the second user adopting only bits, on a bit-by-bit basis, having the measured value beyond the threshold value which is predetermined;
 - (d) the second user informing the first user that the bits adopted are the n-th bits in the transmitted bit sequence, not telling the values of the bits; and
 - (e) the first and second users taking the adopted bits as a key string, and discarding the remaining bits.

PRIOR ART

The prior art reference of record relied upon by the Examiner in rejecting the appealed claims is:

Mayers

US 6,678,379 B1

Jan. 13, 2004

REJECTIONS

Claims 1-6 stand rejected under 35 U.S.C. 102(e) as being anticipated by Mayers.

Rather than reiterate the conflicting viewpoints advanced by the Examiner and the Appellant regarding the above-noted rejection, we make reference to the Examiner's Answer (mailed Nov. 9, 2006) for the reasoning in support of the rejection, and to Appellant's Brief (filed Jun. 19, 2006) for the arguments thereagainst.

OPINION

In reaching our decision in this appeal, we have given careful consideration to Appellant's Specification and claims, to the applied prior art reference, and to the respective positions articulated by Appellant and the Examiner. As a consequence of our review, we make the determinations that follow.

ANTICIPATION

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Analysis of whether a claim is patentable over the prior art under 35 U.S.C. § 102 begins with a determination of the scope of the claim. We determine the scope of the claims in patent applications not solely on the basis of the claim language, but upon giving claims their broadest reasonable construction in light of the specification as it would be interpreted by one of ordinary skill in the art. *In*

re Am. Acad. of Sci. Tech. Ctr., 367 F.3d 1359, 1364, 70 USPQ2d 1827, 1830 (Fed. Cir. 2004). The properly interpreted claim must then be compared with the prior art.

"It is well settled that a prior art reference may anticipate when the claim limitations not expressly found in that reference are nonetheless inherent in it. 'Under the principles of inherency, if the prior art necessarily functions in accordance with, or includes, the claimed limitations, it anticipates'." *In re Cruciferous Sprout Litig.*, 301 F.3d 1343, 1349, 64 USPQ2d 1202, 1206 (Fed. Cir. 2002) (citations and internal quotation marks omitted). "Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient." *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1951 (Fed. Cir. 1999) (citations and internal quotation marks omitted).

"[A] prima facie case of anticipation [may be] based on inherency." *In re King*, 801 F.2d 1324, 1327, 231 USPQ 136, 138-39 (Fed. Cir. 1986). Once a prima facie case of anticipation has been established, the burden shifts to the Appellant to prove that the prior art product does not necessarily or inherently possess the characteristics of the claimed product. *In re Best*, 562 F.2d 1252, 1255, 195 USPQ 430, 433-34 (CCPA 1977) ("Where, as here, the claimed and prior art products are identical or substantially identical, or are produced by identical or substantially identical processes, the PTO can require an applicant to prove that the prior art products do not necessarily or inherently possess the characteristics of his claimed product."). *See also In re Spada*, 911 F.2d 705, 708-09, 15 USPQ2d 1655, 1657-58 (Fed. Cir. 1990).

Appellant argues that Mayers discloses a method for testing the security of a quantum cryptographic system used for quantum key distribution. Appellant argues that Mayers method utilizes polarization states of photons with the photons possessing quantum states satisfying certain relationships between three bases (Br. 6). Appellant argues that the presently claimed invention concerns a key arrangement method including a first system that encodes a bit sequence and sends it to a second system (Br. 7). The second system decodes the received signals and measures the signal values. In contrast to the Mayers's system, in the presently claimed invention, the second system records some second values, which are above a predetermined value, and tells the first system the bit positions of the selected bits (Br. 7). The first system selects values corresponding to those bit positions, and discards the rest of the values (Br. 7). Appellant argues that in comparing the present invention to Mayers, it is clear that Mayers does not adopt only bits having a measured value beyond a threshold value (Br. 7). Appellant argues that as disclosed in Mayers, if a sufficient number of bits meet a parity test, it is concluded that there is no eavesdropping activity. The bits that have been tested or discarded in a shared key is produced from the remaining random series of bits (Br. 7). Appellant argues that in contrast, and as recited in claim 1, the second system adopts only those bits having a measured value beyond the threshold value, and informs the first system of the bit positions of the selected bits. The adopted bits are then used as a key string for the first and second systems (Br. 7). Appellant argues that Mayers discloses instead to discard the bits that are actually tested, and utilize the remaining random series of bits to form a shared key (Br. 7-8), and that in the present invention, it is the second

system that determines which bits to use for the key string. Appellant argues that in contrast, Mayers discloses that the parity of the measurement results are collated on a bitwise basis between the sending and receiving parties (Br. 8). Thus, both the sending and receiving parties in Mayers are involved in the testing procedure (Br. 8).

At the Oral Hearing on September 11, 2007, Appellant's representative argued that the system of Mayers is based on quantum levels which do not use a threshold value. Appellant argued that the photon is either present or not present. Therefore, no threshold value is used in the determination of which bit positions are used.

The Examiner maintains that the term "measuring the decoded signal" is not defined in Appellant's Specification (Answer 5). The Examiner maintains that Mayers determines the bits which correspond to predetermined four sets of bases, and these bits are kept and the other bits are discarded. The Examiner maintains that this implies adopting bits having a measured value beyond a threshold value which is predetermined (Answer 5).

We agree with the Examiner that Mayers teaches a determination of the presence or absence of a photon which corresponds to a predetermined set of bases and those bits are measured. We find the language of independent claim 1 to be broad enough to read on the determination of the presence of a photon and that those bits would be adopted on the bit-by-bit basis as taught by Mayers. Mayers additionally discloses that "about half the bits will correspond to cases where the selected bases constitute one of the abovementioned four sets of bases; these bits are kept, and the other bits are discarded." (Mayers col. 9, ll. 23-26). We find this to be a teaching of

adopting only the bits having a measured value beyond a threshold value. Therefore, Appellant's arguments are not persuasive.

With respect to Appellant's argument concerning both the sending and receiving parties in Mayers being involved in the testing procedure, the Examiner maintains that the claim language is open ended and does not specifically exclude the sending party in the determination (Answer 6). We agree with the Examiner that the language of independent claim 1 does not preclude the involvement of the sending party. Therefore, Appellant's argument is not persuasive, and we will sustain the rejection of independent claim 1 since Appellant has not shown error in the Examiner's initial showing of anticipation. Additionally, we will sustain the rejection of dependent claim 3 which Appellant has not provided separate arguments for patentability.

With respect to dependent claim 2, Appellant argues that "claim 2 recites that if transmission is considered safe, the key string is accepted and refined, for instance. The Examiner cites column 8, line[] 65 through column 9, line[] 20, but the undersigned could not find any teaching of the combination of features of claim 2." (Br. 8). We do not find this to be a separate argument for patentability and is not persuasive. But, in the Reply Brief, Appellant expands upon the original broad argument set forth in the Brief and argues that the cited portions of Mayers do not teach "obtaining a refined key string with amplification such as an error correction process." (Reply Br. 2). We agree with Appellant that the cited portions of Mayers do not discuss the use of amplification or an error correction process. Therefore, we will not sustain the rejection of dependent claim 2 since the

Examiner has not set forth a sufficient initial showing that all the claimed steps are taught by Mayers.

With respect to dependent claim 4, Appellant argues that there was no mention of noise, let alone mutual modulated noise, by another transmitter in the teachings of Mayers (Br. 8). The Examiner maintains that Mayers teaches transmitting signals through a classical public channel which "inherently" implies that the second user uses a receiver affected by mutual modulated noise by another transmitter (Answer 6). We disagree with the Examiner that the public channel would "inherently" be affected by mutual modulated noise in the transmission of the photons as taught by Mayers. We find no support for the Examiner's assertion. Therefore, we will not sustain the rejection of dependent claim 4 since the Examiner has not set forth an initial showing that all the claimed steps are taught by Mayers.

With respect to dependent claims 5 and 6, Appellant argues that Mayers does not disclose the recited limitations regarding the second user determining the threshold value of step (c), considering at least three factors; transmission rate, transmission error rate and degree of security (Br. 8). We agree with the Appellant that the Examiner has not shown that Mayers teaches the recited three factors, and the Examiner merely relies on the teaching of measuring a threshold value (Answer 6-7). Since we find that the Examiner has not made the requisite initial showing that the recited three factors are taught by Mayers, we will not sustain the rejection of dependent claims 5 and 6.

CONCLUSION

To summarize, we have sustained the rejection of independent claim 1 and dependent claim 3 under 35 U.S.C. § 102, and we have not sustained the rejection of dependent claims 2 and 4-6 under 35 U.S.C. § 102.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a).

AFFIRMED-IN-PART

tdl/ce

BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404